uFR aes tester - console application

Version 1.0

Link : https://www.d-logic.net/code/nfc-rfid-reader-sdk/ufr-ds-examples-c_sharp-console

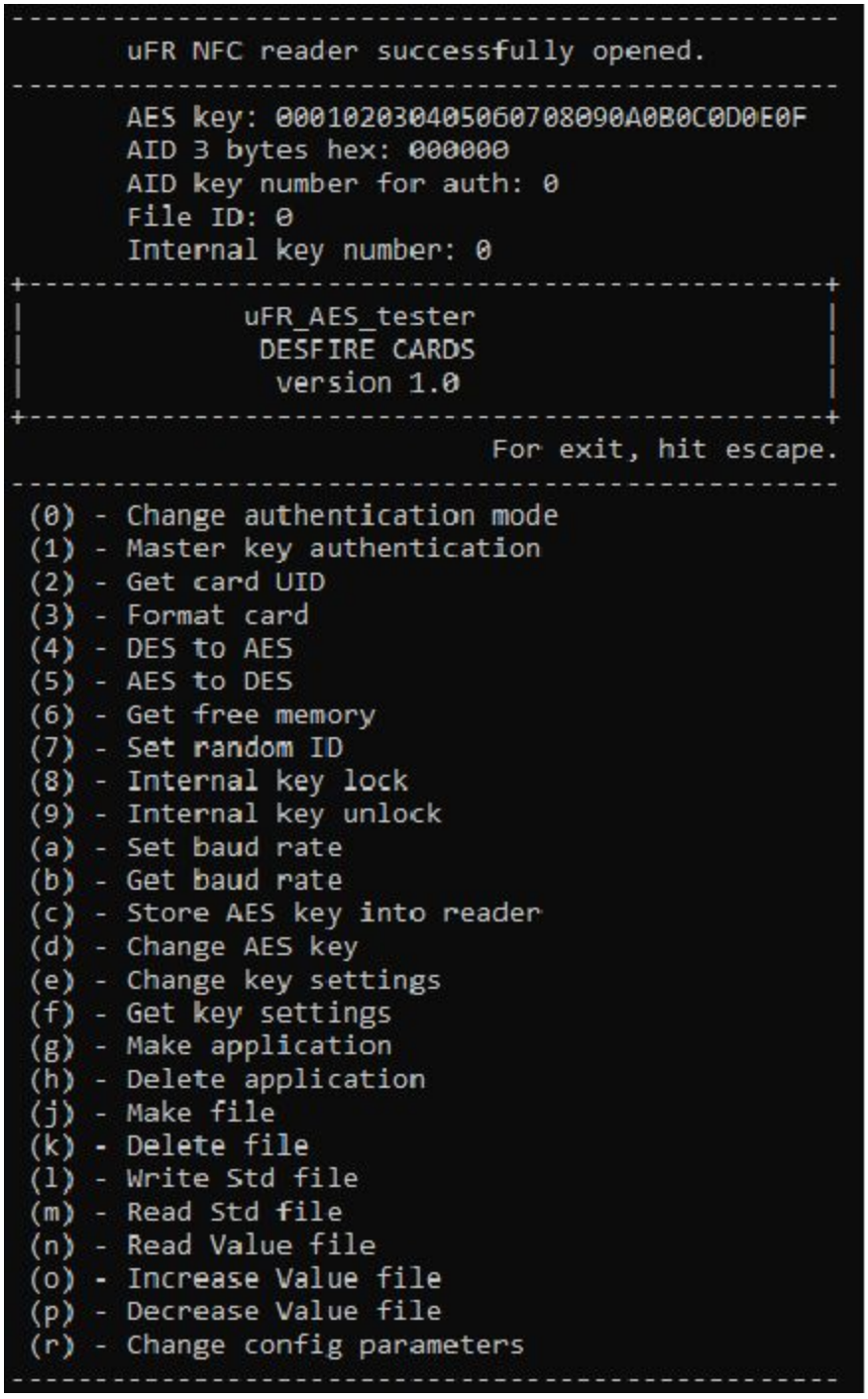
Table of contents

Title	Page number
Application overview	4
Config file explanation (config.txt)	5
Change authentication mode	5
Master key authentication	5
Get card UID	6
Format card	6
DES to AES	7
AES to DES	7
Get free memory	7
Set random ID	7
Internal key lock	7
Internal key unlock	8
Set baud rate	8
Get baud rate	9
Store AES key into reader	9
Change key settings	9
Get key settings	10
Make application	10
Delete application	11
Make file	11

Delete file	13
Write std data file	13
Read std data file	14
Read value file	15
Increase value file	16
Decrease value file	17
Change config parameters	18
Revision history	20

Application overview

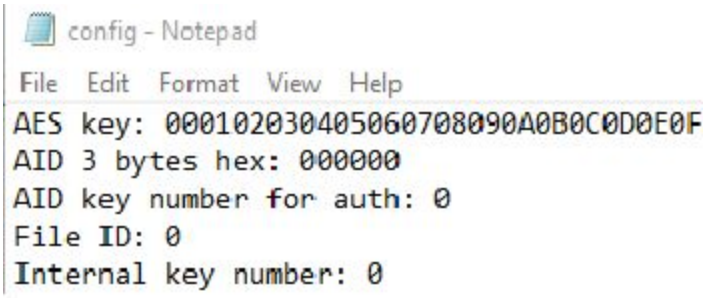
When you start application, it looks like this:



AES key for authentication, AID, AID key number for authentication, File ID and internal key index are read out from config.txt file.

Config file explanation (config.txt)

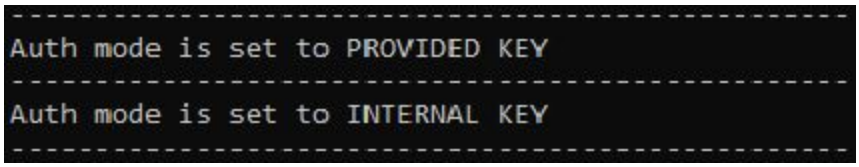
Config file is main folder after you download application from git. In config file you can modify AES key for authentication, AID, AID key number for authentication, File ID or internal key. These parameters are mandatory for applications work with DESFIRE cards.



AES key must be 16 bytes hex - 32 characters in config.txt
AID must be 3 bytes hex.
AID key, File ID, and Internal key are stored as one decimal number depends on index.

(0) - Change authentication mode

For switching between internal or provided key authentication, press '0' on keyboard.
It looks like this (here is '0' pressed twice):



Default authentication is with internal key (key stored into reader).

(1) - Master key authentication

For switching between master key authentication, press '1' on keyboard.
It looks like this (here is '1' pressed twice):

```
------------------------------------------------
Master key authentication is now required
------------------------------------------------
Master key authentication is not required
------------------------------------------------
```

Master key authentication is not required by default.

(2) - Get card UID

Press '2' to get card UID printed on the screen. If your authentication mode is set to INTERNAL, then key stored into reader and key stored into card will be compared. If your authentication mode is set to PROVIDED, then application will look for AES key in config.txt file.

Reading card's UID looks like:

```
Operation completed
Function status is UFR_OK
Card status is CARD_OPERATION_OK
Execution time : 113 ms
Card UID : 04:88:1D:02:8B:51:80
------------------------------------------------
```

(3) - Format card

Pressing number '3' on your keyboard will cause formatting card (deleting all applications and files except AID with number: 000000). Depends on which authentication mode you chose, it will look for AES key into reader (INTERNAL KEY) or in config.txt file (PROVIDED KEY).

Formatting card preview:

```
------------------------------------------------
Operation completed
Function status is UFR_OK
Card status is CARD_OPERATION_OK
Execution time : 517 ms
------------------------------------------------
```

(4) - DES to AES

The new key type becomes AES, and new value of key is 0x00000000000000000000000000000000 (16 zeros).

(5) - AES to DES

Key is returned to card factory value.

(6) - Get free memory

It will print free memory available on card.
It looks like this:

```
------------------------------------------------
Operation completed
Function status is UFR_OK
Card status is CARD_OPERATION_OK
Execution time : 60 ms
Free memory : 2304 bytes
------------------------------------------------
```

(7) - Set random ID

Activating the random ID card options by Set Random ID button. Required authentication using card master key.
The card returns 4 bytes random ID instead 7 bytes unique ID.
Warning: this operation is irreversible.
When this option is activated, the UID can be read by special command that requires authentication using valid key.

(8) - Internal key lock

You have to enter password (8 characters length) to lock keys enrollment.

```
 Input password (8 characters):
11111111
 Operation completed. Status is UFR_OK
```

Keys are now locked with password "11111111".

(9) - Internal key unlock

To unlock the possibility to enroll keys into reader, you must enter the same password to unlock keys which is entered to lock keys enrollment.

```
 Input password (8 characters):
11111111
 Operation completed. Status is UFR_OK
```

It looks the same as keys locking option.

(a) - Set baud rate

After activating the option 'Set baud rate' by pressing 'a' on keyboard you will see multiple choices to choose for transceive and receive baud rate. Just enter the number next to option you want to choose.

```
 Chose number for transceive baud rate :
 0 - 106 kbps
 1 - 212 kbps
 2 - 424 kbps
 3 - 848 kbps
0
 Chose number for receive baud rate :
 0 - 106 kbps
 1 - 212 kbps
 2 - 424 kbps
 3 - 848 kbps
0
 Operation completed. Status is UFR_OK
```

Transceive and receive baud rate are now set to 106 kbps.

Attention: uFR readers series support baud rates up to and including 424 kbps.

(b) - Get baud rate

Reading baud rates looks like:

```
------------------------------------------------
Operation completed. Status is UFR_OK
TX baud rate = 106 kbps
RX baud rate = 106 kbps
------------------------------------------------
```

(c) - Store AES key into reader

For storing the AES key into reader you have to enter key index and 16 bytes AES key.

Example:

```
------------------------------------------------
 Input aes key number (0 - 15) :
0
 Input aes key (16 bytes hex) :
000102030405060708090A0B0C0D0E0F
 Operation completed. Status is UFR_OK
------------------------------------------------
```

Key at index 0 in card is now set to this 16 bytes hex value:
00112233445566778899AABBCCDDEEFF

(e) - Change key settings

For changing key settings, carefully read available settings and chose one. Take care about setting you chose, some of them cannot be changeable anymore.
If you are changing settings for AID 000000 - IT CAN'T BE FORMATTED.

(f) - Get key settings

For getting key settings, press 'f' on keyboard.
Output will be :

```
------------------------------------------------
Operation completed
Function status is UFR_OK
Card status is CARD_OPERATION_OK
Execution time : 107 ms
4 - Settings not changeable anymore and create or
------------------------------------------------
```

You will be able to see number and description of previously chosen setting.

(g) - Make application

For making application, first you need to set master key authentication by pressing '1' on keyboard, you will see output "Master key authentication is now required" as shown on the picture below, then press 'g' and enter AID number (3 bytes hex) you want to create, for example "000001", after choosing AID number you have to choose one of available applications key settings and application will be created.

```
------------------------------------------------
Master key authentication is now required
------------------------------------------------
Input aid number (3 bytes hex) :
000001
Input maximal key number :
1
Choose applications key setting :
0 - No settings
1 - Settings not changeable anymore
2 - Create or delete application with master key au
3 - Master key not changeable anymore
4 - Settings not changeable anymore and create or c
5 - Settings and master key not changeable anymore
6 - Create and delete application with master key a
7 - Settings not changeable anymore, create or dele
    master key is not changeable anymore
2
Operation completed
Function status is UFR_OK
Card status is CARD_OPERATION_OK
Execution time : 139 ms
------------------------------------------------
```

(h) - Delete application

For deleting application, just enter the AID number you want to delete, for example, we will delete the application we created in the previous picture:

```
------------------------------------------------
 Input aid to delete (3 bytes hex) :
000001
 Operation completed
 Function status is UFR_OK
 Card status is CARD_OPERATION_OK
 Execution time : 126 ms
------------------------------------------------
```

Application with AID number 000001 is now deleted.

(j) - Make file

For making file we must create the application first, for example with AID number 000001.
After that, press 'r' to change config parameters (config.txt) and set AES key to 16 bytes with 00 value - enter 32 zeros and AID number to 000001 because we need that settings for authentication for creating file.

```
------------------------------------------------
Current config:
       AES key: 00000000000000000000000000000000
       AID 3 bytes hex: 000001
       AID key number for auth: 0
       File ID: 0
       Internal key number: 0
1 - Change aes key
2 - Change AID
3 - Change AID key number for auth
4 - Change File ID
5 - Change internal key number
esc - Exit to main menu
```

After we set AES key to 16 bytes with 00 and AID to 000001, we must press '0' to change authentication mode from INTERNAL to PROVIDED key because our key for application is now:
00000000000000000000000000000000

Now, press 'j' to make file.

First you have to choose file ID, for example '0'.
Then choose communication mode, for example enter '1' for PLAIN communication mode.
Then choose between standard data file or value file, we will choose standard data file for this example.
Choose read, write, read/write and change key number in range of available indexes for work with file.
At the end, enter file size in bytes, in this example we will enter 20 bytes:

```
-------------------------------------------------
Auth mode is set to PROVIDED KEY
-------------------------------------------------
Input file ID:
0
Chose communication mode:
1. PLAIN
2. MACKED
3. ENCHIPERED
1
Chose file type:
1. Standard data file
2. Value file
1
Input read key number (0 - 15) :
0
Input write key number (0 - 15) :
0
Input read/write key number (0 - 15) :
0
Input change key number (0 - 15) :
0
Input size of file (bytes) :
20
Operation completed
Function status is UFR_OK
Card status is CARD_OPERATION_OK
Execution time : 134 ms
-------------------------------------------------
```

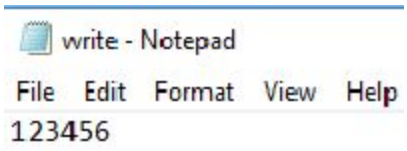
The standard data file is successfully created.

(k) - Delete file

For deleting file just enter file ID you want to delete.

(l) - Write std data file

In file write.txt which is also in the main folder like config.txt we will put numbers from 1 - 6 for example.



Then choose communication mode and file will be written into card.

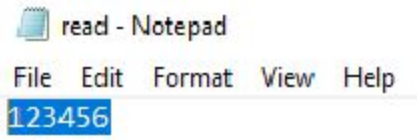
```
------------------------------------------------
Chose communication mode:
1. PLAIN
2. MACKED
3. ENCHIPERED
1
Operation completed
Function status is UFR_OK
Card status is CARD_OPERATION_OK
Execution time : 111 ms
------------------------------------------------
```

(m) - Read std data file

Press 'm' for reading std data file, first we choose communication mode and then we choose number of bytes we want to read. In the previous example we write numbers from 1 - 6 in write.txt file so we will now choose 6 bytes to read.

```
-------------------------------------------------
 Chose communication mode:
 1. PLAIN
 2. MACKED
 3. ENCHIPERED
1
 Input file length to read (bytes):
6
 Operation completed
 Function status is UFR_OK
 Card status is CARD_OPERATION_OK
 Execution time : 109 ms
-------------------------------------------------
```

Navigate to read.txt file in the main folder and you should see text like this:



File is successfully read.

(n) - Read value file

For reading value file we must create it first. We will press '3' to format card and create another application and new file again. This time file type will be VALUE FILE.

1. Set master key authentication
2. Create application
3. Change config parameters and set AES key to: 00000000000000000000000000000000
4. Set authentication mode to PROVIDED KEY
5. Make value file

```
 Chose file type:
 1. Standard data file
 2. Value file
2
 Input read key number (0 - 15) :
0
 Input write key number (0 - 15) :
0
 Input read/write key number (0 - 15) :
0
 Input change key number (0 - 15) :
0
 Input lower limit :
0
 Input upper limit :
200
 Input value :
50
 Do you want to enable limited credit?
 1. Enabled
 2. Disabled
2
 Do you want to use free get value?
 1. Use free get value
 2. Don't use free get value
2
 Operation completed
 Function status is UFR_OK
 Card status is CARD_OPERATION_OK
 Execution time : 138 ms
```

We will set lower limmit to 0, upper limit to 200, and value to 50.
After value file is created we can read its value.

Press 'n' to read value:

```
------------------------------------------------
Chose communication mode:
1. PLAIN
2. MACKED
3. ENCHIPERED
1
Operation completed
Function status is UFR_OK
Card status is CARD_OPERATION_OK
Execution time : 107 ms
Value : 50
------------------------------------------------
```

Value is 50 as we expected.

(o) - Increase value file

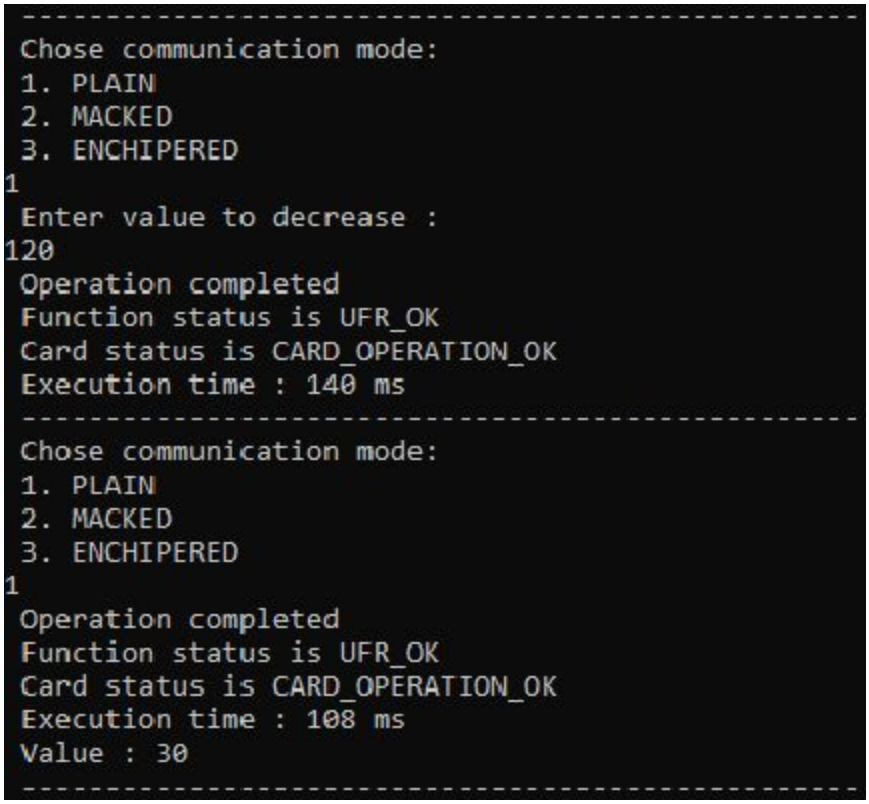
We will press 'o' to increase our value for 100 and then press 'n' to read value again:

```
------------------------------------------------
Chose communication mode:
1. PLAIN
2. MACKED
3. ENCHIPERED
1
Enter value to increase :
100
Operation completed
Function status is UFR_OK
Card status is CARD_OPERATION_OK
Execution time : 140 ms
------------------------------------------------
Chose communication mode:
1. PLAIN
2. MACKED
3. ENCHIPERED
1
Operation completed
Function status is UFR_OK
Card status is CARD_OPERATION_OK
Execution time : 107 ms
Value : 150
------------------------------------------------
```

Value is now increased for 100, current value is 150.

(p) - Decrease value file

We will press 'p' to decrease our value for 120 and then press 'n' to read value again:



Value is now decreased for 120, current value is 30.

(r) - Change config parameters

Press 'r' to change config.txt file.
First, you will see current config.txt file with options 1 - 5 for changing and esc for back to main menu.

```
Current config:
        AES key: 00000000000000000000000000000000
        AID 3 bytes hex: 000001
        AID key number for auth: 0
        File ID: 0
        Internal key number: 0
1 - Change aes key
2 - Change AID
3 - Change AID key number for auth
4 - Change File ID
5 - Change internal key number
esc - Exit to main menu
```

For example, lets change AID and File ID
First press '3' and enter new AID and then press '4' and enter new File ID:

```
2 Input new AID (3 bytes hex):
000001
 Current config:
        AES key: 00000000000000000000000000000000
        AID 3 bytes hex: 000001
        AID key number for auth: 0
        File ID: 0
        Internal key number: 0
 1 - Change aes key
 2 - Change AID
 3 - Change AID key number for auth
 4 - Change File ID
 5 - Change internal key number
 esc - Exit to main menu
4 Input new File ID:
1
 Current config:
        AES key: 00000000000000000000000000000000
        AID 3 bytes hex: 000001
        AID key number for auth: 0
        File ID: 1
        Internal key number: 0
 1 - Change aes key
 2 - Change AID
 3 - Change AID key number for auth
 4 - Change File ID
 5 - Change internal key number
 esc - Exit to main menu
```

Now press 'r' again to read the changes.

```
Current config:
       AES key: 00000000000000000000000000000000
       AID 3 bytes hex: 000001
       AID key number for auth: 0
       File ID: 1
       Internal key number: 0
1 - Change aes key
2 - Change AID
3 - Change AID key number for auth
4 - Change File ID
5 - Change internal key number
esc - Exit to main menu
```

AID number and FIle ID are successfully changed. The same thing happened in config.txt file:

config - Notepad

File Edit Format View Help

```
AES key: 00000000000000000000000000000000
AID 3 bytes hex: 000001
AID key number for auth: 0
File ID: 1
Internal key number: 0
```

Revision history

Date	Version	Comment
2019-04-09	1.0	Base document